?? Wazuh Logs Advanced Log Troubleshooting (with JQ)

The Wazuh Dashboard logs are JSON-formatted, but standard `journalctl` prepends timestamps that break JSON parsers. Use these commands to see perfectly formatted, readable logs.

1

View Pretty-Printed JSON

The `-o cat` flag removes the OS timestamps, allowing `jq` to parse the dashboard's internal JSON correctly.

```
sudo journalctl -u wazuh-dashboard -o cat -f | jq '.'
```

2

Extract Only Timestamps and Messages

If you want a very clean list of just the time and the action being performed, use this `jq` filter.

```
sudo journalctl -u wazuh-dashboard -o cat -f | jq -r '"[\(."@timestamp")] \(
.message)"'
```

3

Handling Non-JSON Errors

Sometimes the system outputs non-JSON errors (like service start failures). If the commands above fail, fall back to the raw log.

```
sudo journalctl -u wazuh-dashboard -e --no-pager
```

Resulting Output

By using `-o cat`, you ensure that every line passed to `jq` starts with `{`, eliminating the `parse error` you encountered.

Revision #2
Created 2026-01-01 17:21:41 UTC by joliveira
Updated 2026-01-01 17:22:17 UTC by joliveira